UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,046	04/08/2004	Marshall Beddoe	FNDSTN.032A	9634

7590 03/26/2008

ZIKA-KOTAB
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
RUTTEN, JAMES D	

ART UNIT	PAPER NUMBER
2192	

MAIL DATE	DELIVERY MODE
03/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/821,046	BEDDOE ET AL.	
	Examiner	Art Unit	
	JAMES RUTTEN	2192	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7-12-04, 1-12-06, 5-16-06, 7-16-07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 is directed to an "operating system identification system." The elements of the system appear to be directed to a system of software, and are considered to be functional descriptive material. Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality

to be realized, and is thus statutory. Claims 2-15 are rejected as being dependent upon claim 1 but failing to remedy the deficiencies of parent claim 1. Likewise, independent claim 16 is rejected for the same reasons as claim 1, and dependent claims 17-23 are rejected as being dependent upon, and failing to remedy the deficiencies of parent claim 16.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7-9, 11, 12, 16, 17, 19, 20, 39, and 41-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record "Remote OS detection via TCP/IP Stack FingerPrinting" by Fyodor ("Fyodor") in view of U.S. Patent Application Publication US 2002/0138605 A1 by Canis et al. ("Canis").

Fyodor generally discloses the *nmap* operating system identification tool which identifies operating systems by fingerprinting networking stacks.

In regard to claim 1, Fyodor discloses:

An operating system identification system comprising:

an identification module configured to execute a plurality of operating system identification tests, each operating system identification test configured to make an identification of an operating system being executed by a network node; See page 8:

> I have created a reference implementation of the OS detection techniques mentioned above (except those I said were excluded). I have added this to my Nmap scanner which has the advantage that it already knows what ports are open and closed for fingerprinting so you do not have to tell it. It is also portable among Linux, *BSD, and Solaris 2.51 and 2.6, and some other operating systems.

a plurality of identification rules configured to define a procedure by which the identification module makes an overall identification of the operating system, wherein the overall identification is based at least in part on at least one of the identifications made by the plurality of operating system identification tests; See at least page 11:

> We use the command:
> nmap -sS -F -o transmeta.log -v -O www.transmeta.com//24
>
> This says SYN scan for known ports (from /etc/services), log the results to 'transmeta.log', be verbose about it, do an OS scan, and scan the class 'C' where www.transmeta.com resides. …

This passage shows that identification rules are used which define the procedure of identification. Identification rules define how the command produces the identification.

Fyodor does not expressly disclose: *and a conflict resolution module configured to detect at least one of a plurality of cases defined by a plurality of conflict resolution definitions in which at least some of the plurality of operating system identification tests disagree in their identification of the operating system, and configured to, upon detecting such a case, to make an identification of the operating system and to cause the identification module to modify the overall identification based at least on the identification made by the conflict resolution module.*

However, Canis teaches that when two tests provide conflicting identification, conflict resolution defines the overall identification. See paragraph [0043]:

> Specifically, collection tool C1 may have collected information that conflicts with information collected by collection tool C2. For example, collection tool C1 may have identified a different address for workstation W1 than did collection tool C2. To resolve such conflicts, analysis system 46 preferably includes conflict resolution rules 48. Rules 48 may dictate, for example, that in the event of a conflict between collection tools C1 and C2, collection tool C1 "prevails."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Canis' conflict resolution with Fyodor's fingerprinting in order to resolve identification conflicts as suggested by Canis.

In regard to claim 2, the above rejection of claim 1 is incorporated. Fyodor further discloses: *wherein the plurality of operating system identification tests includes a Transmission Control Protocol identification test*. See bottom of page 4, e.g. "TCP ISN Sampling."

In regard to claim 3, the above rejection of claim 2 is incorporated. Fyodor further discloses: *wherein the plurality of operating system identification tests further includes an Internet Control Message Protocol identification test*. See page 6, e.g. "ICMP Message Quoting."

In regard to claim 4, the above rejection of claim 3 is incorporated. Fyodor further discloses: *wherein the plurality of operating system identification tests further includes a banner matching test*. See bottom of page 2, e.g. "banner."

In regard to claim 5, the above rejection of claim 4 is incorporated. Fyodor further discloses: *wherein the plurality of operating system identification tests further includes an open port signature test*. See page 11, e.g. "scan for known ports."

In regard to claims 7-9, the above rejection of claim 1 is incorporated. All further limitations have been addressed in the above rejections of claims 3-5, respectively.

In regard to claim 11, the above rejection of claim 4 is incorporated. Fyodor further discloses: *a plurality of identification fingerprints, each identification fingerprint configured to associate an operating system with responses expected to be generated by the associated operating system in response to execution of one of the identification tests, wherein the identification made by each identification test is based, at least in part, on comparisons between the identification fingerprints and actual responses generated by a tested operating system in response to execution of one of the identification tests*. See at least page 4, e.g. "Fingerprinting Methodology."

In regard to claim 12, the above rejection of claim 11 is incorporated. Fyodor further discloses: *a logic engine, wherein the logic engine performs the comparisons between the identification fingerprints and actual responses*. See middle of page 4: "probe for the differences."

In regard to claim 16, all limitations have been addressed in the above rejections of claims 1-4.

In regard to claims 17, 19, and 20, the above rejection of claim 16 is incorporated. All further limitations have been addressed in the above rejection of claims 5, 11, and 12, respectively.

In regard to claim 39, all limitations have been addressed in the above rejection of claim 1 and the following rejection of claim 33.

In regard to claims 41 and 42, the above rejection of claim 39 is incorporated. All further limitations have been addressed in the above rejection of claim 16.

In regard to claims 43 and 44, the above rejection of claim 39 is incorporated. All further limitations have been addressed in the above rejections of claims 4 and 5.

6. Claims 6, 10, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fyodor and Canis as applied to claims 1, 5, and 17 above, and further in view of Paul Asadoorian, "NetBios Null Sessions: The Good, The Bad, and The Ugly" ("Asadoorian").

In regard to claim 6, the above rejection of claim 5 is incorporated. Fyodor does not expressly disclose: *wherein the plurality of operating system identification tests further includes a NULL session enumeration test*. However, Asadoorian discloses that Windows operating systems permit the Null Sessions which can be exploited using the "enum" tool. See page 1. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Asadoorian's teaching of Null Sessions with Fyodor's tests in order to identify Windows operating systems that are subject to this vulnerability as suggested by Asadoorian.

In regard to claim 10, the above rejection of claim 1 is incorporated. All further limitations have been addressed in the above rejection of claim 6.

In regard to claim 18, the above rejection of claim 17 is incorporated. All further limitations have been addressed in the above rejection of claim 6.

7. Claims 13 and 21 rejected under 35 U.S.C. 103(a) as being unpatentable over Fyodor and Canis as applied to claims 1 and 5 above, and further in view of U.S. Patent No. 6,519,703 to Joyce ("Joyce").

In regard to claim 13, the above rejection of claim 12 is incorporated. Fyodor and Canis does not expressly disclose: *wherein at least one of the comparisons performed by the logic engine is a fuzzy logic comparison.* However, Joyce discloses using fuzzy logic in analyzing a rule base. See column 2 lines 22-24, e.g. "fuzzy logic." It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Joyce's teaching of fuzzy logic with Fyodor's rules in order to provide adaptability as suggested by Joyce.

In regard to claim 21, the above rejection of claim 20 is incorporated. All further limitations have been addressed in the above rejection of claim 13.

8. Claims 14, 15, 22-27, 29, 30, 32-37, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fyodor and Canis as applied to claims 4 and 16 above, and further in view of U.S. Patent No. 6,618,717 to Karadimitriou et al. ("Karadimitriou").

In regard to claim 14, the above rejection of claim 4 is incorporated. Fyodor and Canis does not expressly disclose: *wherein each identification of the operating system made by one of the identification tests is associated with a confidence level indicating a degree to which the identification is deemed to be accurate, and wherein the overall identification is further based on the confidence level associated with the at least one identification relied upon to make the overall identification.* However, Karadimitriou teaches identification associated with a confidence level of accuracy based upon test results. See column 8 lines 40-49. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Karadimitriou's confidence level with Fyodor's tests in order to provide the highest level of probability of an accurate identification as suggested by Karadimitriou.

In regard to claim 15, the above rejection of claim 14 is incorporated. Karadimitriou further discloses: *wherein each associated confidence level represents a probability that the identification is accurate.* See Karadimitriou column 8 lines 46-49. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the references for the same reasons provided in the above rejection of claim 14.

In regard to claims 22 and 23, the above rejection of claim 15 is incorporated. All further limitations have been addressed in the above rejection of claims 14 and 15, respectively.

In regard to claim 24, Fyodor discloses method of identifying an operating system executed by a network node. See at least page 4, e.g. "Fingerprinting Methodology." All further limitations have been addressed in the above rejections of claims 1-4 and 14.

In regard to claim 25, the above rejection of claim 24 is incorporated. Fyodor further discloses: *wherein the network node is one of a computer, a router, and a printer.* See at least the middle of page 2, e.g. "router."

In regard to claim 26, the above rejection of claim 24 is incorporated. Fyodor further discloses: *wherein transmitting at least a first plurality of Internet Control Message Protocol packets further includes transmitting at least a first User Datagram Protocol packet to the network node and receiving in response at least a second User Datagram Protocol packet,* See at least the top of page 6, e.g. "UDP." All further limitations have been addressed in the above rejection of claim 24.

In regard to claim 27, the above rejection of claim 24 is incorporated. All further limitations have been addressed in the above rejection of claim 5.

In regard to claims 29 and 30, the above rejection of claim 27 is incorporated. All further limitations have been addressed in the above rejections of claims 1 and 5.

In regard to claim 32, Fyodor discloses:

A method of identifying an operating system executed by a network node. See at least page 4, e.g. "Fingerprinting Methodology."

...

Fyodor does not expressly disclose: *assessing, based at least on one characteristic of each identification of the operating system returned by the plurality of tests, which of the tests to select for determining an overall identification of the operating system;* However, Karadimitriou teaches an overall identification based upon assessment of a plurality of tests. See column 8 lines 46-49:

> Having a probability/confidence level 58 assigned to each candidate name 40, it is straightforward then to choose the candidate name 40 with the highest probability of being the Web site's 42 content owner name.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Karadimitriou's assessment with Fyodor's fingerprinting in order to provide the highest level of probability of an accurate identification as suggested by Karadimitriou.

All further limitations have been addressed in the above rejection of claim 1.

In regard to claim 33, the above rejection of claim 32 is incorporated. All further limitations have been addressed in the above rejection of claim 1. Note that the aggregated results can be reasonably broadly interpreted as Canis' information as stored in database 26 (see paragraph [0043]).

In regard to claim 34, the above rejection of claim 32 is incorporated. Fyodor further discloses: *wherein each of the tests returns an identification of an operating system that is not influenced by the identification returned by any of the other tests.* See at least page 2 "Classical Techniques."

In regard to claim 35, the above rejection of claim 32 is incorporated. Fyodor further discloses: *wherein the plurality of tests includes at least a first test in which the returned identification of an operating system is generated based on at least connecting to at least one open port on the network node and transmitting to the open port data configured to cause the open port to return at least one banner*. See the telnet example at the bottom of page 2.

In regard to claims 36 and 37 the above rejection of claim 35 is incorporated. All further limitations have been addressed in the above rejections of claims 5 and 14, respectively.

In regard to claim 40, the above rejection of claim 39 is incorporated. All further limitations have been addressed in the above rejection of claim 14.

9. Claims 28 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fyodor, Canis, and Karadimitriou as applied to claim 27, and further in view of "Winfingerprint Scan Options" ("Winfingerprint").

In regard to claim 28, the above rejection of claim 27 is incorporated. Fyodor, Canis and Karadimitriou does not expressly disclose: *determining whether NULL session access is available on at least one port configured to run at least one of a Server Message Block service and a NETBIOS service, and if such NULL session access is available, using such NULL session access to determine at least a major version and a*

minor version of the operating system executed by the network node, and generating, based on the major version and the minor version, a fifth identification of which operating system is executed by the network node and a fifth confidence level indicating a degree to which the fifth identification is deemed accurate, wherein generating the overall identification of the operating system is further based on the fifth identification and the fifth confidence level. However, Winfingerprint discloses using NULL session access and SMB queries while determining major and minor OS version. See page 1. All further limitations have been addressed in the above rejection of claim 24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the techniques of Winfingerprint with the fingerprinting of Fyodor in order to determine OS as suggested by Fyodor.

In regard to claim 45, the above rejection of claim 44 is incorporated. All further limitations have been addressed in the above rejection of claim 28.

10. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fyodor, Canis, and Karadimitriou as applied to claim 27, and further in view of "Request for Comments 793" by DARPA ("RFC 793") as incorporated by reference in paragraph [0031] on page 15 of the originally filed specification.

In regard to claim 31, the above rejection of claim 27 is incorporated. Fyodor, Canis, and Karadimitriou do not expressly disclose: *wherein the first plurality of Transmission Control Protocol packets are compliant with a specification of*

Transmission Control Protocol packets defined by DARPA Request for Comments 793. However, as pointed out in paragraph [0031] on page 15 of the originally filed specification, RFC 793 defines a standard for TCP packets. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the standard of RFC 793 in order to comply with commonly accepted standards.

11. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fyodor, Canis, and Karadimitriou as applied to claim 37, and further in view of WIPO International Publication No. WO 03/107321 A1 by Jordahl ("Jordahl").

In regard to claim 38, the above rejection of claim 37 is incorporated. Fyodor, Canis, and Karadimitriou do not expressly disclose: *wherein at least one confidence level concerning whether an operating system identification is correct is determined using a fitness calculation.* However, Jordahl discloses using a fitness function to determine confidence levels. See Abstract, e.g. "fitness functions." It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Jordahl's fitness function with Karadimitriou's confidence level in order to determine a threshold confidence level as suggested by Jordahl.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES RUTTEN whose telephone number is (571)272-3703. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Q. Dam can be reached on (571)272-3695. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. Derek Rutten/
Patent Examiner, Art Unit 2192